

EXHIBIT C

DUPLICATE

FILED IN CHAMBERS

OCT 23 2014

(USAO GAN 6/10) Search Warrant

United States District Court
NORTHERN DISTRICT OF GEORGIA

U.S. MAGISTRATE JUDGE
N D. GEORGIA

In the Matter of the Search of

Information associated with csdesign22@yahoo.com that is stored at premises owned, maintained, controlled, or operated by Yahoo! Inc., an email provider headquartered at 701 First Avenue, Sunnyvale, California 94089

**APPLICATION AND
AFFIDAVIT FOR
SEARCH WARRANT**
Case number: 1:14-MC-973

UNDER SEAL

I, Jacqueline Reynolds, being duly sworn depose and say:

I am a Special Agent of the Internal Revenue Service Criminal Investigation and have reason to believe that on the property described as:

SEE ATTACHMENT A

there is now concealed certain information and certain data, namely,

SEE ATTACHMENT B

which constitutes evidence of the commission of a criminal offense and property which has been used as the means of committing a criminal offense, concerning violations of Title 18, United States Code, Sections 1341 (mail fraud), 1343 (wire fraud), 1001 (false statements) and 371 (conspiracy), over which the United States District Court for the Northern District of Georgia has jurisdiction. The facts to support a finding of Probable Cause are as follows:

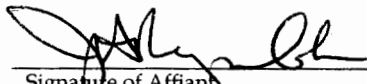
SEE ATTACHED AFFIDAVIT

Continued on attached sheet made a part hereof.

Sworn to before me, and subscribed in my presence

October 23, 2014
Date

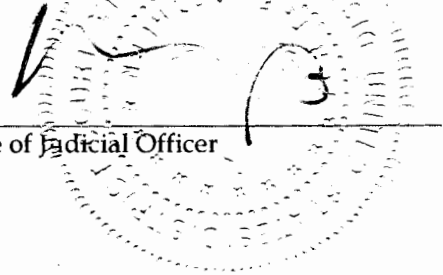
ALAN J. BAVERMAN
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer
AUSA Steven D. Grimberg
(2014R00345)



Signature of Affiant
Jacqueline Reynolds

Atlanta, Georgia

City and States



Signature of Judicial Officer

AFFIDAVIT

I, Jacqueline Reynolds, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Yahoo, an email provider headquartered at 701 First Avenue, Sunnyvale, California 94089. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo to disclose to the government records and other information in its possession pertaining to the subscribers or customers associated with the account, including the contents of communications.

2. I am a Special Agent with Internal Revenue Service-Criminal Investigation and have been since August 1991. I am currently assigned to the Atlanta Field Office. My duties and responsibilities as a Special Agent include the investigation of alleged criminal violations of Title 26, Title 18 and Title 31 of the United States Code. I am a graduate of the Federal Law Enforcement Training Center where I received extensive training on the different aspects of criminal investigations. I have received training relating to the enforcement of United States tax laws, including the investigation of tax evasion schemes, money laundering, conspiracies to defraud the United States, and other criminal matters. I have also received training in the United States laws relating to the judicial process, probable cause, the Fourth Amendment, searches, seizures, and the forfeiture of property, goods, and currency to the United States. As a Special Agent with IRS-CI, I have received training in financial investigative techniques and accounting.

I have also attended several seminars taught by various agencies, including the Department of Justice and the Department of Treasury. I have been trained to conduct criminal investigations, particularly with respect to locating and acquiring evidence of criminal activity. I have been the affiant for numerous search warrant applications and have personally led criminal investigations leading to the convictions of many individuals. Some of these investigations have involved individuals who have communicated through the use of e-mail messages and these e-mail messages have been important evidence in the prosecutions of these individuals.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that the email account csdesign22@yahoo.com, which is the subject of this search warrant, will contain evidence concerning violations of Title 18, United States Code, Sections 1341 (mail fraud), 1343 (wire fraud), 1001 (false statements) and 371 (conspiracy).

PROBABLE CAUSE

5. Hi-Tech Pharmaceuticals, Inc. ("Hi-Tech") is a domestic corporation registered with the Georgia Secretary of State Corporations Division. According to records filed with the Georgia Secretary of State, Jared Wheat is the sole officer of Hi-Tech. The principal address of Hi-Tech is located in Norcross, Georgia. Hi-Tech manufactures dietary supplements under the Hi-Tech brand name as well as private label names.

6. As a manufacturer of dietary supplements, Hi-Tech is required to comply with Good Manufacturing Practices (GMPs) pursuant to Title 21, Code of Federal Regulations, Section 111. Some customers of Hi-Tech require proof of Hi-Tech's compliance with GMPs in order to conduct business. Evidence of a firm's compliance with GMPs can be accomplished by providing a copy of a valid GMP Certification issued by an independent and qualified firm.

7. On May 17, 2013, the Honorable Magistrate Judge Linda T. Walker signed a federal search warrant for the email account htpharmac@aol.com, which was an account known to have been utilized by Jared Wheat, the sole officer of Hi-Tech. Law enforcement agents have reviewed email communications obtained from the search warrant, which include retained email communications sent and/or received by Choat Soviravong, an employee of Hi-Tech who performed graphic art and design work, through the email address csdesign22@yahoo.com. The emails that have been reviewed indicate that Jared Wheat may have been directing Choat Soviravong to prepare false and fraudulent GMP Certifications, which were subsequently transmitted to customers and potential customers of Hi-Tech.

8. For example, on or about March 3, 2011, an email was sent to htpharmac@aol.com, an email address known to have been used by Jared Wheat, from Bobbie Vachon, a person believed to be a customer or potential customer of Hi-Tech, with the subject line - RE: Health Canada. The email stated in part, "Jared, In order to add Hi-Tech Pharmaceuticals to our site license I will require one of the following forms of documentation for evidence that you comply with GMP regulations." Within a few hours of receiving the above email, an email was sent to htpharmac@aol.com from csdesign22@yahoo.com with the subject line-Certificate and attachment-Pharmatech Certification March2011.pdf. The email stated in

part, "Here is the file. Thanks, Chot S.-Graphic Coordinator." The attachment is an unsigned certificate purportedly issued by PharmaTech Consulting, Inc. indicating that Hi-Tech Pharmaceuticals has been found to be in compliance with GMP requirements. Pharmatech Consulting, Inc. is a company that was founded by Jared Wheat and known to be affiliated with Hi-Tech. The purported certificate was dated December 3, 2010 and had an initial certification date of December 3, 2011. The purported certificate listed its certification number as PT-12310.

9. On or about March 15, 2011, an email was sent from htpharmac@aol.com to csdesign22@yahoo.com with the subject line- I will be back there in a minute and attachment- auditCARReport.pdf. The attachment is a copy of a GMP Registration Annual Audit Corrective Action Report prepared by NSF International for Hi-Tech based upon a GMP Audit performed by NSF in November 2010. NSF International is an independent firm which performs GMP audits for dietary supplement manufacturers. Records obtained from NSF International have confirmed that NSF was contracted by Hi-Tech to perform a GMP Registration Audit, however, NSF International did not certify Hi-Tech Pharmaceuticals as compliant with GMPs.

10. On or about March 28, 2011, an email was sent from esteveesspartan@gmail.com, a person believed to be a customer or potential customer of Hi-Tech, to htpharmac@aol.com, with the subject line-Joe from Canada. The email stated in part, "Thanks for the info on the GMP audit-I will speak with my Q & A person and get back to you."

11. In May 2014, information was received from Health Canada, a federal department with the Canadian government, that a Canadian firm submitted site licensure paperwork to add Hi-Tech to its site license. In particular, the Canadian firm submitted a copy of a purported GMP Certificate issued by PharmaTech Consulting dated December 5, 2012 with

an initial certification date of December 3, 2010. The purported certificate listed its certification number as PT-12310. In addition to the purported GMP Certificate, the Canadian firm submitted a copy of a purported GMP audit report of Hi-Tech performed by PharmaTech in November 2012. The purported audit report is very similar in content and design to the GMP Registration Annual Audit issued by NSF to Hi-Tech in December 2010. However, the name of the auditor and date of the audit changed to personnel purportedly associated with PharmaTech. Additionally, all of the audit findings NSF found to be "Not Acceptable" had been changed to "Acceptable".

12. On or about July 5, 2012, an email was sent from mark.mcleod@vpxsports.com, a person believed to be a customer or potential customer of Hi-Tech, to htpharmac@aol.com, with the subject line-Documentation Needed. The email stated in part, "Jared, I need the following from Hi-Tech: 2. Copy of any 3rd party license for example, AIB, NSF." On or about July 17, 2012, an email was sent from htpharmac@aol.com to mark.mcleod@vpxsports.com with subject line-Documentation and attachment-Pharmatech GMP_registration_annual_audit.xlsx, which stated in part, "Here is our last audit." The attachment is a copy of a purported GMP audit report of Hi-Tech by PharmaTech in December 2012. The purported audit report is very similar in content and design to the GMP Registration Annual Audit issued by NSF to Hi-Tech Pharmaceuticals, Inc in December 2010. However, the name of the auditor and date of the audit changed to personnel purportedly associated with PharmaTech. Additionally, all of the audit findings NSF found to be "Not Acceptable" had been changed to "Acceptable".

13. Based upon the investigation to date, I believe there is probable cause to believe that Hi-Tech submitted false and fraudulent GMP certificates and false and fraudulent GMP

audit reports to customers and potential customers. Based upon my training and experience, such documents are generally prepared by persons technically capable of creating and modifying text and images, such as persons with a graphics design background. The investigation has discovered that Choat Soviravong has the background and expertise to manipulate documents in this manner, and that there is probable cause to believe that his email account at csdesign22@yahoo.com will contain evidence of these criminal offenses.

14. In June 2014, I interviewed Soviravong concerning his employment at Hi-Tech. Soviravong stated he had been employed with Hi-Tech since 2005 as a graphics designer. Soviravong's duties include designing product labels, product boxes and marketing materials. Soviravong stated he believed he is the only person employed at Hi-Tech who performs graphics design work. Soviravong stated he has and continues to utilize the email account of csdesign22@yahoo.com to conduct business activities for Hi-Tech. Soviravong further stated he utilizes the email account of csdesign22@yahoo.com to communicate with Jared Wheat for work-related correspondence. Soviravong denied preparing any GMP certifications or GMP Audit Reports.

15. A preservation request, dated June 24, 2014, was sent to Yahoo requesting the e-mail activity for the e-mail account csdesign22@yahoo.com be preserved. A second preservation request was sent to Yahoo on September 4, 2014, requesting preservation for an additional 90 days.

16. In my training and experience, I have learned that Yahoo provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Subscribers obtain an account by registering with Yahoo. During the registration process, Yahoo asks

subscribers to provide basic personal information. Therefore, the computers of Yahoo are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Yahoo subscribers) and information concerning subscribers and their use of Yahoo services, such as account access information, e-mail transaction information, and account application information.

17. In general, an e-mail that is sent to Yahoo subscriber is stored in the subscriber's "mail box" on Yahoo servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Yahoo servers indefinitely.

18. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Yahoo's servers, and then transmitted to its end destination. Yahoo often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Yahoo server, the e-mail can remain on the system indefinitely

19. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Yahoo but may not include all of these categories of data.

20. A Yahoo subscriber can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Yahoo.

21. Subscribers to Yahoo might not store on their home computers copies of the e-mails stored in their Yahoo account. This is particularly true when they access their Yahoo

account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

22. In general, e-mail providers like Yahoo ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

23. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Yahoo's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

24. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support

services, as well as records of any actions taken by the provider or user as a result of the communications.

25. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mails in the account, and attachments to e-mails, including pictures and files.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Yahoo to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

27. Based on the foregoing, I request that the Court issue the proposed warrant.

28. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States... that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

30. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness. Although the above documents may be sealed, it is respectfully requested that the data obtained as a result of the search warrant may be disclosed to third parties to facilitate analysis.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the e-mail account utilizing the e-mail address: csdesign22@yahoo.com that is stored at premises owned, maintained, controlled, or operated by Yahoo, a company headquartered at 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by YAHOO

To the extent that the information described in Attachment A is within the possession, custody, or control of Yahoo, Yahoo is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- d. All records pertaining to communications between Yahoo and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of mail fraud, wire fraud, false statements, and conspiracy to commit any of the foregoing, including but not limited to the following matters:

- a. Audit reports, certificates(including GMP certificates), and any other communications, representations or documents concerning Hi-Tech's compliance with FDA rules and regulations.
- b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Yahoo, and my official title is _____. I am a custodian of records for Yahoo. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Yahoo, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Yahoo; and
- c. such records were made by Yahoo as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature